# CVE Detail – CVE-2022-1509

Command Injection Vulnerability in GitHub repository hestiacp/hestiacp prior to 1.5.12. An authenticated remote attacker with low privileges can execute arbitrary code under root context.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.81392

## CVSS Scoring

CVSS v3.1 Score: 9.9

Severity: CRITICAL

## Mapped CWE(s)

* CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

## CAPEC(s)

* CAPEC-136: LDAP Injection
* CAPEC-15: Command Delimiters
* CAPEC-183: IMAP/SMTP Command Injection
* CAPEC-248: Command Injection
* CAPEC-40: Manipulating Writeable Terminal Devices
* CAPEC-43: Exploiting Multiple Input Interpretation Layers
* CAPEC-75: Manipulating Writeable Configuration Files
* CAPEC-76: Manipulating Web Input to File System Calls

## Affected Products

* cpe:2.3:a:hestiacp:control\_panel:\*:\*:\*:\*:\*:\*:\*:\*